ADMINISTRATIVE MANUAL

SUBJECT: INFORMATION TECHNOLOGY Security Policies and Rules	*Chapter:* 24
	Section: 24.2
REFERENCES: 24.3 Access Request Rules and Processes	*Page:* 1 of 7
	Revised: 12-28-2006

SECURITY POLICIES AND RULES

I. PURPOSE:

The purpose of this document is to inform all users of Department of Health and Senior Services (DHSS) applications, resources, and networks; their responsibilities; and DHSS information technology security policies and rules.

II. SCOPE: Departmentwide

III. QUALIFYING STATEMENTS:

DHSS uses access controls and other security measures to protect the confidentiality, integrity, and availability of the information handled by its technology (computer and communication) systems.

DHSS has legal ownership of the contents of all files stored on its technology systems. Therefore, the DHSS maintains the authority to: (1) restrict or revoke any user's privileges; (2) inspect, audit, copy, remove, or otherwise alter any data, program, or computer that may undermine these objectives; and (3) take any other steps deemed necessary to manage and protect its information systems.

This authority may be exercised with or without notice to the involved users. By making use of DHSS systems, users consent to allow all information they store on DHSS systems to be divulged to law enforcement at the discretion of DHSS management and should have no expectation of privacy associated with the information they store in or send through these systems. Only the DHSS Deputy Department Director may grant exceptions to this policy.

IV. SECURITY POLICIES AND RULES:

All users of the DHSS information technology systems will abide by the following security rules.

A. DHSS ACCESS PRIVILEGES

1. The technology system privileges of all users, systems, and programs will be restricted based on a job-related, need-to-know basis. The user may share data with others having authorized access via network drives, computers, or the DHSS Intranet.

2. The division/center directors will establish specific written protocols regarding the categories of people who will be granted permission to access various types of electronic information for which their division/center is responsible. These protocols must specify information use limitations by those to whom access is granted.

3. Division or Center Directors will appoint Local Security Officers (LSO) and a Program Security Officers (PSO). These delegated officers will be given authority to approve, edit, or deny requests for access. (Refer to Policy 24.3 Section IV.)

4. The LSO must assure that users sign a Confidentiality Agreement, which includes a statement regarding confidentiality of computer data, prior to approving a user's request for an ID that allows access to DHSS systems and that the user renews this Agreement annually.

5. Each computer will have one person identified as the primary user of that computer, but multiple users may have accounts on a single computer. The primary user must be aware of the existence of other user accounts and the ability of the other users to view all files and make changes while logged into their accounts on the shared computer.

B. ACCESS ID REQUIREMENTS

1. User IDs will be granted to specific users only after they have completed the transaction in the DHSS Automated Security Access Program (ASAP) and that request has been approved by the user's LSO and/or PSO (see Administrative Manual 24.3). If the user also requests access to a DHSS database, the designated representative (PSO) of the division, center or

bureau responsible for the data to be accessed must approve the access request.

2. Users will be granted access to a single computer, specified in their ASAP request unless other computers are identified.

C. USER RESPONSIBILITIES

1. Users will automatically be logged off DHSS Information Technology Services Division (ITSD) developed applications if they have had no activity for a specified time. The time may vary depending on the confidentiality level of the data, but will never exceed thirty (30) minutes.

2. Users must not leave their networked computer unattended without first logging out, locking the workstation, or using a screen saver that requires a password to access the network and/or computer operating system.

3. Every user will have one concurrent network login access by default. Users must submit an ASAP network request for additional access with a statement of reasons for the need for additional concurrent network login connections. Unlimited network connections will not be granted.

4. Every user will have network login access time restrictions. Default login access is permitted daily between the hours of 4:00 AM and 11:00 PM. Users must submit an ASAP network request for 24-hour login access.

5. Users are responsible for all activity performed with their personal user IDs. User IDs must not be utilized by anyone but the individuals to whom the ID has been issued. Users must not allow others to perform any activity with their user IDs. Similarly, users must not perform any activity with IDs belonging to other users.

D. PASSWORDS

1. Every user must have a unique user ID and a personal secret password. User IDs and passwords are required for access to the DHSS network and applications.

2. The initial password issued by a security administrator is only valid for the user's first on-line session. At that time, the user must choose another password before any other work can be done.

3. Passwords must never be divulged or shared with anyone else besides the authorized user. To do so exposes the authorized user to responsibility for actions that the other party takes with the password. If users need to share computer resident data, they must not allow another person to use their user ID and password.

4. All passwords must have at least five characters. All user-chosen passwords for the network and electronic applications must be difficult to guess. Words in a dictionary, derivatives of a user's ID, and common character sequences such as "123456" and "abcde" must not be employed. Likewise, personal details such as spouse's name, license plate, social security number, and birthday must not be used unless accompanied by additional unrelated characters.

5. Users must not construct passwords made up of a certain number of characters that do not change combined with a certain number of characters that predictably change. For example, users must not employ passwords like "WICJAN" in January, "WICFEB" in February, etc.

6. Passwords will not be displayed within the password entry box and cannot be printed.

7. All users must change their passwords at least once every sixty (60) days. Passwords must not be written down and left in a place where unauthorized persons might discover them.

8. To prevent password guessing attacks, the number of consecutive attempts to enter an incorrect password is limited. After three unsuccessful attempts to enter a password, the user ID involved will be suspended until reset by a DHSS ITSD network administrator after the user contacts the DHSS ITSD Help Desk.

9. Users must promptly change their password(s) if they have any reason to think the password(s) may have been disclosed.

10. All users may be instructed to change their password(s) if the DHSS ITSD network administrator believes the system security has been compromised.

11. Passwords must not be stored in applications (such as by turning on the "remember my password" feature), so that access can be made to the DHSS systems without entering the password each time. Where possible, the feature allowing, "remember my password" must be disabled at the system level.

E. RESOURCES

1. All transportable computing devices, and computers located outside the offices of DHSS (such as those used for remote access or telecommuting) shall meet or exceed the requirements identified in the DHSS Technology Standards document.

2. DHSS ITSD must approve all wireless technology and wireless network installations. Acceptable equipment and configurations are covered in the DHSS Technology Standards document.

3. All computing devices used for remote access or telecommuting shall only be configured by DHSS ITSD technicians and must have an operating system password.

4. Because DHSS ITSD must approve user access and all computing devices used for Virtual Private Networking (VPN) remote access must be configured to DHSS Technology Standards to use a VPN connection, an ASAP Request is required.

5. Only DHSS computing devices will be allowed to connect to any DHSS equipment or the DHSS network. Non-DHSS computing devices are allowed to access web mail through an Internet connection.

6. Information regarding access to DHSS computer and communication systems, such as dial-up modem phone numbers, is considered confidential. This information must not be posted on electronic bulletin boards, listed in telephone directories, placed on business cards, placed on websites, or otherwise made available to third parties without the written permission of the DHSS ITSD Chief Information Officer. Electronic mail addresses are permitted.

F. RESIGNATIONS

1. Before a user leaves any position with DHSS, his/her network-resident files must be promptly reviewed by his/her bureau or office chief to determine who should become the custodian of such files, and/or the appropriate methods to be used for file disposal. Notification of the decision must be communicated by means of an ASAP request to document and authorize the requested action. In the event of an immediate termination of an employee, the employee's manager must contact the DHSS ITSD Help Desk to secure resources then follow up with an ASAP request.

2. Read-only rights can be granted to another valid user for up to five (5) workdays on E-mail accounts of users no longer employed by DHSS. This proxy access will be enabled only after they have completed an ASAP request and approved by the user's Local Security Officer (LSO) and/or Program Security Officer (PSO). (See Administrative Manual 24.3) All other existing proxies for that user ID will be deleted. An extension up to five (5) days can be granted upon receipt of an additional ASAP request. No extensions will be granted beyond the ten workdays.

3. All user IDs will automatically have their associated access privileges revoked after a forty-two (42) workday period of inactivity.

4. All DHSS information systems access privileges for a user ID will be promptly terminated at the time DHSS ITSD is informed that a worker ceases to provide services to DHSS.

5. Prior to a user's last day of work, supervisors must submit an ASAP request to delete or lock that person's system privileges.

Prepared By:

Director
Information Technology Services Division

Approved By:

Deputy Department Director

SUBJECT: INFORMATION TECHNOLOGY Information Security Incident Reporting	*Chapter:* 24
	Section: 24.7
REFERENCES: Administrative Manual Policies 24.2 Security Policies and Rules 24.3 Access Request Rules and Processes	*Page:* 1 of 4
	Revised: 12-28-2007

INFORMATION SECURITY INCIDENT REPORTING

I. PURPOSE:

This policy establishes a Department of Health and Senior Services (DHSS) Information Security Incident Reporting process and identifies the procedures, roles and responsibilities needed for its implementation. The purpose is to minimize the damage from security incidents and to prevent their recurrence.

II. SCOPE:

This policy applies to all DHSS workforce members, including all employees, contractors, interns, trainees, researchers, and volunteers. DHSS information systems include computers connected to DHSS local, statewide, and Internet communication networks, database storage systems, electronic records systems, imaging systems, e-mail systems, and other computing devices such as Personal Digital Assistants (PDAs), laptops or stand-alone PCs.

III. POLICY:

The DHSS will implement an Information Security Incident Reporting Program to report any event that violates the integrity, confidentiality, or availability of its computer information systems, applications, and data. The goal is to ensure prompt recovery of affected systems; minimize the possible impact of the incident in terms of data loss, corruption, or system disruption; prevent further attacks or damages; and address any legal issues.

SUBJECT: INFORMATION TECHNOLOGY Information Security Incident Reporting	*Chapter:* 24
	Section: 24.7
REFERENCES: Administrative Manual Policies 24.2 Security Policies and Rules 24.3 Access Request Rules and Processes	*Page:* 2 of 4
	Revised: 12-28-2007

IV. PROCEDURES:

A computer security incident is any adverse event that compromises some aspect of computer or network security, resulting in a loss of confidentiality, integrity, or availability of information.

A. Workforce members must report the following security incidents to the DHSS Information Technology Services Division (ITSD) Help Desk or the DHSS ITSD Security Officer immediately:

1. Destruction or tampering with data;
2. Unauthorized disclosure of information;
3. Loss or theft of information or hardware;
4. Disruption or denial of service;
5. Unauthorized use of or access to computer systems or information;
6. Damage or unauthorized changes to systems or hardware;
7. Compromise of secret password; and/or
8. Discovery of malicious code, including but not limited to worms, viruses, Trojans, spyware, and website defacement.

In addition, laptop loss or theft must also be reported to division management and the Director's Office.

B. Workforce members must provide specific information so the technical staff will be able to respond to the incident efficiently and effectively, including but not limited to:

1. Contact name, location, email and phone number.
2. Description of the incident.
3. Any equipment, networks, systems and users involved or affected.
4. Actions taken by user, internal technical staff or outside parties.

C. Technical staff or security officers may take the following actions:

1. Isolate equipment from the network;
2. Examine files and logs;
3. Interview affected system users;
4. Take custody of equipment for further investigation;
5. Issue notices or warnings to affected users or to DHSS;
6. Contact the Division/Center or DHSS executive management; and
7. Contact law enforcement agencies.

Any incident that impacts the computing environment with the potential to affect other State agencies or systems outside of DHSS immediate control will be reported to the Office of Administration, Information Security Management Office.

D. The DHSS ITSD Help Desk or DHSS ITSD Security Officer must be notified immediately of any security incident that results in a significant loss or corruption of data, unauthorized disclosure of confidential information, or disruption of service to multiple users.

V. ENFORCEMENT:

DHSS workforce members who fail to comply with this policy are subject to disciplinary actions. These actions may include dismissal, depending on the severity of the offense, and possible legal action.

Prepared By:

Director
Information Technology Services Division

Approved By:

Deputy Department Director

ADMINISTRATIVE MANUAL

SUBJECT: INFORMATION TECHNOLOGY Laptop and Portable Computer Security Policy	*Chapter:* 24 *Section:* 24.14
REFERENCES: 24.2 Security Policies and Rules 24.5 Information Technology Use Policy, Guidelines and Processes 24.14A Laptop Custodial Agreement	*Page:* 1 of 5 *Revised:* 12-28-2007

LAPTOP AND PORTABLE COMPUTER SECURITY POLICY

I. PURPOSE:

The purpose of this policy is to protect Department of Health and Senior Services (DHSS) laptop computers and other portable computing devices such as Personal Data Assistants (PDAs), including Blackberries; and to inform all users of such devices of their responsibilities in securing these devices.

II. SCOPE:

Departmentwide.

III. QUALIFYING STATEMENTS:

The term "laptop" will be used in this document to mean any laptop, tablet, notebook, handheld, or portable computer device, including PDAs. The theft or loss of, or damage to DHSS laptop computers is of increasing concern. There is a substantial financial impact arising from the cost of replacement, as well as costs associated with data replacement, lost productivity, procurement, and set-up. There is also a serious risk associated with the exposure or loss of any sensitive, unique or personal information the device may contain.

To counter these risks, laptop security must be addressed by users and management understanding their responsibilities, and through physical security and access controls.

IV. USER RESPONSIBILITIES:

All users of DHSS laptop and portable computer devices will abide by the following rules:

SUBJECT: INFORMATION TECHNOLOGY Laptop and Portable Computer Security Policy	*Chapter:* 24 *Section:* 24.14
REFERENCES: 24.2 Security Policies and Rules 24.5 Information Technology Use Policy, Guidelines and Processes 24.14A Laptop Custodial Agreement	*Page:* 2 of 5 *Revised:* 12-28-2007

A. General Use:

1. Laptop users must agree to take responsibility for the security of the laptop assigned to them and the information it contains.

2. Upon allocation of the laptop, the custodian must complete a "Laptop Custodian Agreement" and undertake to comply with all applicable sections of this Laptop Security Policy. The Laptop Custodian Agreement is attached to this policy as 24.14A. In the case of a shared laptop, one custodian must be designated and a sign-out/sign-in sheet must be implemented to track which user has the laptop at all times.

3. Laptops issued to staff remain the property of the DHSS. When the laptop is allocated to the individual, the user assumes temporary "custodianship" of the laptop.

4. Upon leaving the employment of, or cessation of contract work for the DHSS, the individual must return the laptop to his/her manager or supervisor, re-signing their original "Laptop Custodian Agreement." This releases the individual from the responsibility of the "custodianship" of the laptop.

5. Only DHSS approved executable software may be installed on the laptop. Users must take all reasonable steps to protect against the installation of unlicensed or malicious software.

B. Since laptops are more fragile than desktops, the following recommendations on care and maintenance should be followed:

1. When transporting your computer, always shut it down, turn the power off, and put it in a carrying case.

2. Be careful not to bump or drop your computer, do not carry items with it that could harm it.

3. Take care when handling and storing all cables, especially network and modem cables, as they can be damaged easily.

4. Avoid touching the screen.

5. Avoid subjecting the laptop to extreme temperature changes.

6. Keep all food and liquids away from your laptop. Almost any liquid spilt on the computer can result in extremely expensive repairs.

7. Keep diskettes, drives and your computer away from magnetic fields. Magnetic fields can erase data on both diskettes and hard drives.

8. Whenever possible, avoid turning off your laptop when the hard drive light is on because data on the hard drive could be lost or corrupted.

9. Use only the power supply provided with the laptop. There are voltage differences in other power supplies that can limit the life of the laptop.

C. Users must take the following physical security preventative measures:

1. A laptop displaying sensitive information should not be used in a public place, e.g., on a train, aircraft or bus, which would enable others to see the information on the screen.

2. When leaving a laptop unattended in a non-DHSS facility for any extended period, e.g., lunch breaks or overnight, users should physically secure it with a cable lock or lock it in a cabinet or in a private office.

3. In vulnerable situations, e.g. public areas such as airport lounges, hotel lobbies, meeting rooms and conference centers, the laptop must never be left unattended.

4. Portable computers should whenever permitted be carried as hand luggage when traveling.

5. Laptop computers should not be left in an unattended vehicle, even for a short period of time, or left in a vehicle overnight. When impractical, laptops must be out of sight, in an area such as the trunk, and the vehicle locked.

6. Where any of the above rules are either inappropriate or impractical, the owner is responsible for taking all reasonable steps to minimize the risk of loss or damage of the laptop.

D. Users must take the following access control measures:

1. All laptops should be password protected (i.e., password needed to access the computer operating system).

2. Users must select a password in accordance with state Enterprise Architecture and Administrative Policy 24.2 Security Policies and Rules.

3. Users must secure their laptop display with a screen-saver password or lock their computer when left unattended. Laptops should only be left unattended in a secure location, such as the users office, never in a public location, or any other location that would increase the risk of the laptop being lost or stolen.

4. Users must not allow non-DHSS employees to access or use DHSS equipment.

5. Users must not allow non-DHSS employees to service DHSS equipment unless DHSS Information Technology Services Division (ITSD) technicians have approved the service in advance.

6. Users must not connect DHSS laptops to non-DHSS networks, or use them to dial into non-DHSS Internet Service Providers such as America On Line or Socket except those instances where DHSS ITSD has approved the connection (Policy 24.2 Subsection E).

7. Users may not create or modify the user accounts, or modify network protocols on the laptop, unless approved in advance by the DHSS ITSD.

E. Users must take the following measures to protect DHSS data:

1. All sensitive information must be stored on DHSS network servers by default and not copied to the local drive. This ensures that such data is secure and is automatically backed-up as a matter of course.

2. Remote users should connect to the DHSS VPN and save sensitive data to the network.

3. Laptop users must notify the appropriate authorities immediately if their laptop is lost or stolen. Users must immediately advise the local law enforcement and then their manager or supervisor as soon as possible. The user or supervisor/manager must follow the incident reporting procedures in accordance with Policy 24.7 "Information Security Incident Reporting."

V. DHSS MANAGEMENT RESPONSIBILITIES:

The Division or Center Director must ensure that users are fully aware of the security issues and are sufficiently confident in the use of the solutions provided.

Prepared By:

_____

Director
Information Technology Services Division

Approved By:

_____

Deputy Department Director